

by Slater in col 4, lines 32-65, specifically wherein it is stated that a digital certificate of the merchant may be appended to the financial transaction instructions, where the merchant's digital certificate provides additional verification of the merchant's identity and the integrity of the financial transaction instructions, please note that this digital certificate is conveyed from the user or purchaser to the merchant.

The underlining shows that Slater's digital certificate is the merchant's digital certificate (see also Slater, col. 4, lines 60-61), whereas the claimed digital certificate (that is conveyed to the transaction processor via the merchant) is the user's digital certificate.

The Office Action also asserts (see last sentence in page 4, item 5b above) that the merchant's digital certificate originally came from the user. Applicant respectfully disagrees, as the Applicant can find no portion of Slater, col 4, lines 32-65 where this is disclosed.

In Slater, the User's Digital Certificate is Different Than the Merchant's Digital Certificate

The Applicant thanks the Examiner for pointing out that another portion of Slater (col. 8, lines 29-51 – see Office Action, page 4, item 5a) does indeed disclose a user's digital certificate. However, this user's digital certificate is entirely different from the merchant's digital certificate discussed in the previous section (see also Slater, col. 4, lines 32-65 and col. 9, lines 13-64). The former is used in communications between the user and the merchant, for identifying the user to the merchant. The latter is used in communications between the merchant and the financial institution, for identifying the merchant to the financial institution. This is a 2-step security protocol involving conventional digital certificates: first, the user identifies himself to the merchant; and then the merchant identifies himself to the financial institution.¹

The pending claims are directed at a fundamentally different scheme. A special form of user's digital certificate is created that binds the user's public key together with the user's

¹ This is also apparent from the fact that Slater discusses the user's digital certificate in paragraphs covering the user-merchant communication (col. 8, line 29 – col. 9, line 12), and the merchant's digital certificate in later paragraphs covering the user-merchant communication (col. 9, lines 13-64; see also col. 4, lines 32-65).

financial information (see below). This special user's digital certificate is then routed (e.g., through the merchant) to the financial institution to allow the financial institution to directly verify the binding (and thus, to gain assurance as to the user's financial information).

Applicant believes that the Office Action has inadvertently confused Slater's two digital certificates as being the same, whereas they are totally distinct. Accordingly, Applicant respectfully disagrees with, and traverses, this rejection.

Cryptographic Binding is More than Conventional Digital Certification

On page 4, item c, the Office Action states that Slater (col. 4, lines 32-65) discloses a user's digital certificate conveyable to a transaction processor via a merchant. As shown above, the cited portion of Slater pertains to the merchant's digital certificate, not the user's digital certificate.

Even assuming (for the sake of argument) that such digital certificate were the user's digital certificate, its use in Slater is an entirely conventional process involving two distinct and unconnected steps. That is, the owner of the digital certificate would sign (or otherwise encrypt) the financial information with his private key. Then, the signer would send his public key, via his digital certificate, to a recipient. The signed information is in no way bound to the public key, as required by the claims. Rather, the digital signature involves only the private key, and the certificate involves only the public key. In contrast, the claims require that the information and the public key be cryptographically bound together – which is not possible in the conventional approach.

Accordingly, Applicant respectfully disagrees with, and traverses, this rejection.

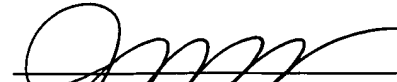
Conclusion

For the reasons given above, Applicant respectfully requests that the rejections be withdrawn and the claims passed to allowance.

The Examiner is invited to call the Applicant's attorney, Joe Yang, at (650) 470-4565.

Respectfully submitted,

Date: January 21, 2003


Joseph Yang
Reg. No. 41, 387

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
525 University Avenue
Palo Alto, California 94301